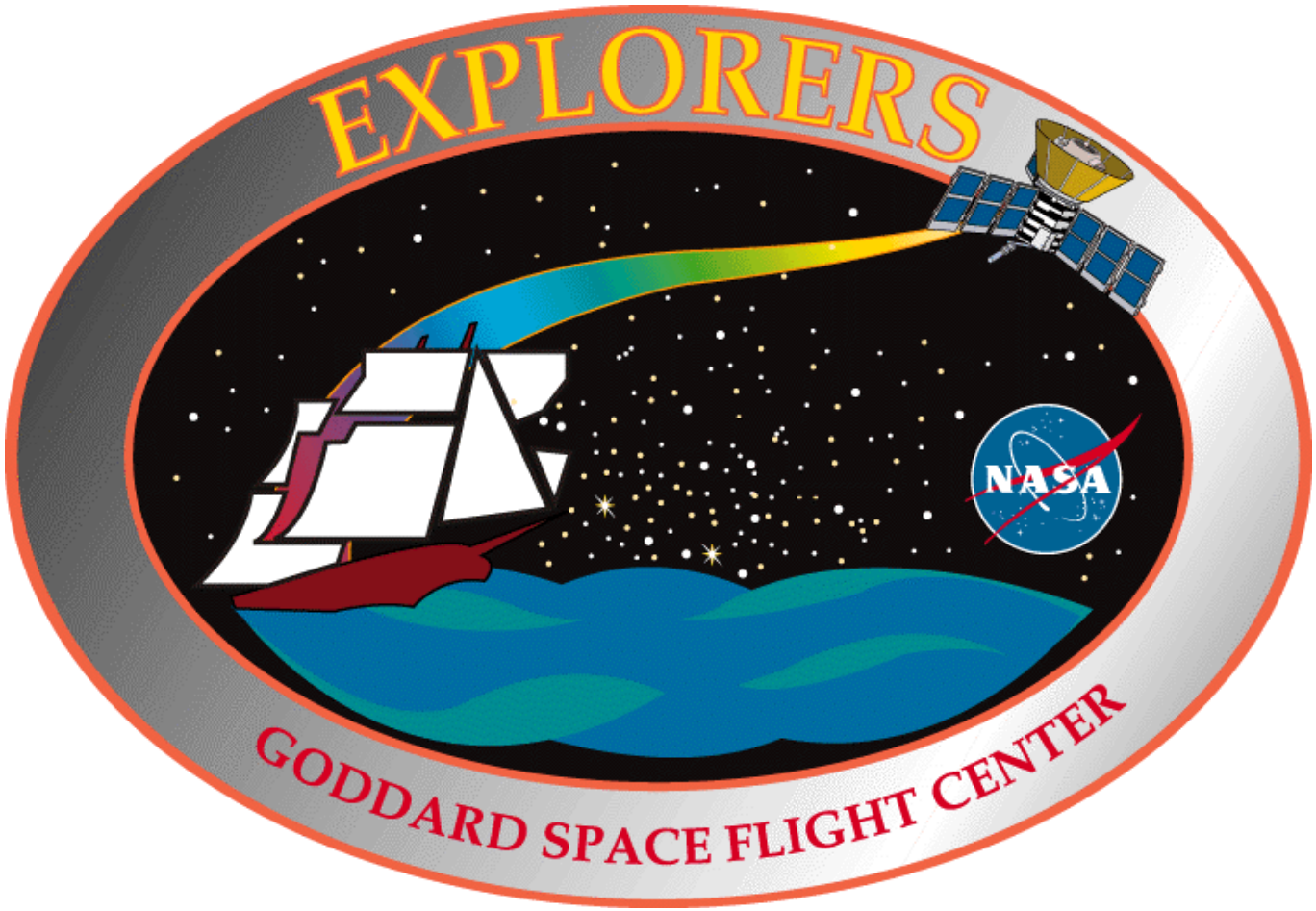
SMEX PI Mode Missions Kickoff Meeting

Safety, Reliability, & Quality Assurance Overview

Rick Claffy, GSFC Code 410/303, X6-7866



SMEX PI Missions Kickoff Meeting SR&QA

- Necessary SR&QA effort is defined by SMEX AO, EPL Reference Document #25 (SMEX SR&QA Requirements)
  - Discusses EXP Program Office & PI joint effort to define best mix of roles and responsibilities for SR&QA execution.
    - Code 410/PI SR&QA Insight Agreement.
      - Becomes part of GSFC/PI Contract as a condition for confirmation.
      - Defines Early the Inter-Institutional Partnering Arrangement for SR&QA services.
    - Drafted by GSFC, negotiated, updated, signed by PI/PM & Explorer PM.

SMEX PI Missions Kickoff Meeting SR&QA

- **Requires PIs to implement a product assurance program that is consistent with ISO 9000 series ANSI/ASQC Q9001-1994.**
  - ISO registration not required, but a significant degree of conformity is expected with the Standard's sections where a good fit exists and it makes sound engineering or programmatic sense.
  - Program must ensure SMEX Safety, Reliability, and Quality Assurance Requirements are met.
  - Tailoring allowed in most assurance technology areas, but …
  - The highly specialized discipline of System Safety is dictated by Air Force EWR 127-1, enforced for NASA via GSFC System Safety Office. Historically, expert guidance through this difficult process has been needed by PI teams.

SMEX PI Missions Kickoff Meeting SR&QA

- **Specifics of PI SR&QA Program to be worked out with Explorers during definition phase.**
  - SMEX SR&QA Requirements are basis for PI SR&QA Program & associated documentation.
  - Working level discussions invited on all SR&QA technology topics.
    - Establish basis for Insight Agreement.
    - Mutual understanding of how implementation will meet requirements.
    - Share historical experience from past PI Mode SMEX missions.
  - PI Quality Manual, PAIP, or equivalent deliverable document to be reviewed by GSFC for approval during Phase B.
- **SMEX SR&QA document Highlights:**
  - Invokes Hi-Reliability Workmanship standards.

SMEX PI Missions Kickoff Meeting SR&QA

- Strongly Urges flight Printed Wiring Board Coupon DPA by certified facility prior to population with flight EEE parts.
- Requires a PI Failure Reporting System for phase C/D/E.
- Lays out Design Review Requirements.
- Details specific System Safety program requirements and deliverables with process flow descriptions (EPL Ref. #25 a-d).
  - Magnitude of System Safety effort must not be under-estimated.
    - Allocate/identify roles & resources.
    - Get the right people.
    - Start early.
  - GSFC can help in numerous ways.
- EEE Parts Selection criteria per GSFC 311-INST-001 or equal.
  - PI shall maintain and review Parts Lists with GSFC.
  - PI shall use an organized system to manage parts application, evaluation, and use.
    - Includes mandatory GIDEP Alert, NASA Advisory, GSFC PMC query responses.

SMEX PI Missions Kickoff Meeting SR&QA

- Materials and Processes program required as typical for GSFC sponsored missions.
- Reliability
  - Risk assessments made and mitigation strategies identified.
  - FMEA at Instrument to Spacecraft interface.
- Software
  - Code to be structured, error free, and maintainable.
  - Establish & document SW requirements, external interface specs, user guides.
  - Internal (peer) and external software design reviews.
- Verification
  - Verification/test program to ensure all mission requirements are met.
  - Documentation to include verification matrix, environments matrix, and test procedures.

SMEX PI Missions Kickoff Meeting SR&QA

- Emergent Themes Directed by NASA HQ since AO release:
  - Red Team within Integrated Independent Review Team.
    - Team expectations can exceed traditional baseline review requirements.
      - Reviewers w/ Extra, detailed questions from Red Team charter.
      - RFA trail & Failure Report closures thoroughly checked by Red Team.
    - GSFC Policy has shifted to Code 301 Chaired Reviews for PI Missions.
  - Reliability Emphasis On:
    - Probabilistic Risk Assessment (PRA).
    - Fault Tree Analysis, etc.
    - FMEA @ subsystem level.
      - Identify all single string design features.
      - Failure Impacts/mitigation.
  - Tangible Continuous Risk Tracking & Management System.
  - Software IV&V.
    - Each mission evaluated for SW complexity/risk/need.
    - Determination of appropriate level of IV&V involvement via standardized criteria.
    - Software Assurance on equal footing w/ hardware.
  - Lessons Learned Information System.

Mission Success is the GSFC Center Director's Ultimate Responsibility to the NASA Administrator.